7-3

УДК 681.3:519.72:003.26

В.К. Задирака, А.М. Кудин
Институт кибернетики им. В.М. Глушкова НАН Украины, г. Киев
Украина, 03680 МСП, г. Киев, проспект Академика Глушкова, 40

Особенности реализации криптографических и стеганографических систем по принципу облачных вычислительных технологий

V.K. Zadiraka, A.M. Kudin
Glushkov Institute of Cybernetic of NAS of Ukraine, c. Kiev
Ukraine, 03187, c. Kiev 40 Glushkova ave.

Features of the Implementation of Cryptosystems and Stegosystems Based on Clouds Computing

В.К. Задірака, А.М. Кудін
Інститут кібернетики ім. В.М. Глушкова НАН України, м. Київ
Україна, 03680 МСП, м. Київ, проспект Академіка Глушкова, 40

Особливості реалізації криптографічних та стеганографічних систем за принципом хмарних обчислювальних технологій

Появление и развитие облачных вычислений определяет новые постановки задач при построении систем защиты информации. Одной из открытых проблем является проблема оценки стойкости криптографических и стеганографических систем, использующихся в облаках, к атакам на реализацию. Существующие методики оценки не в полной мере позволяют решать эту задачу, поэтому в статье предлагается новый метод оценки стойкости к атакам на реализацию, основанный на использовании общей теории оптимальных алгоритмов. Приводятся примеры оценки стойкости к временным атакам на основе предложенного подхода.
Ключевые слова: облачные вычисления, криптосистемы, стеганосистемы,
атаки по побочным каналам, атаки на реализацию, общая теория оптимальных алгоритмов.

The new problems of creation information security systems appeared due to development of cloud computing. One open problem is estimation security of cryptosystems and stegosystems to side-channel attacks. This problem is not solved the existing methods in full. New method based on general theory of optimal algorithms for solving this problem is proposed. Authors makes an examples of estimation security based on this method to timing attacks.
Key words: cloud computing, cryptosystem, stegosystems, side-channel attacks,
general theory of optimal algorithms.

Поява та розвиток хмарних обчислень визначає нові постановки задач при побудові систем захисту інформації. Однією з відкритих проблем є проблема оцінки стійкості криптографічних та стеганографічних систем, які використовуються у «хмарах», до атак на реалізацію. Існуючі методики оцінки не повною мірою дозволяють вирішувати цю задачу, тому у статті запропонований новий метод оцінки стійкості до атак на реалізацію, заснований на загальній теорії оптимальних алгоритмів. Наводяться приклади оцінки стійкості до часових атак на базі запропонованого підходу.
Ключові слова: хмарні обчислення, криптосистеми, стеганосистеми,
атаки за побічними каналами, атаки на реалізацію, загальна теорія оптимальних алгоритмів.

Введение

Основной тенденцией развития информационно-коммуникационных систем (ИКС) последних лет стало широкое использование технологий виртуализации и их развития – облачных вычислительных технологий. Проблеме построения безопасных (для различных определений состояния безопасности информации) облачных систем посвящено достаточно много работ [1-7], однако вопросы системного подхода к проектированию, анализу состояния безопасности и реализации методов и средств защиты информации исследованы эпизодически. Анализ проблем проектирования и реализации криптосистем для облачных ИКС фактически представлен задачами построения гомоморфных криптосистем [7]. Как показано авторами в работах [8-10], проблему необходимо рассматривать в более широком смысле. Действительно, главной особенностью облачных систем, изменяющей постановку задачи по проектированию систем их защиты, является «предоставление вычислительных услуг в требуемом количестве» или «эластичность вычислений» [11]. Обеспечение этого свойства облачных систем требует наличия гибко изменяющейся, распределенной архитектуры построения системы защиты информации, управление которой осуществляет сама облачная система в автоматическом режиме. Для осуществления возможности построения такой системы автоматического управления безопасностью информации требуется построение математических моделей оценки безопасности текущего состояния системы в целом и отдельных ее подсистем.

Целью данной работы является анализ особенности реализации криптосистем и стеганосистем для ИКС, построенных по парадигме облачных вычислений и разработка адекватной математической модели для оценки их стойкости к атакам на реализацию (в частности – атакам по побочным каналам).

Модель угроз для облачных технологий

Модель угроз облачных вычислительных систем наследует все свойства модели угроз распределенных и виртуальных технологий, добавляя при этом новые, специфические типы угроз. К угрозам, наследуемым от виртуальных вычислительных технологий, относятся следующие типы угроз:

– угрозы атак на базовую операционную систему или гипервизор (нарушения безопасности взаимодействия между виртуальными машинами, атаки на интерфейс взаимодействия между виртуальной машиной (ВМ) и гипервизором, атаки непосредственно на гипервизор);

– угрозы атак, направленные на виртуальную машину (нарушение политики безопасности конкретной виртуальной машины для распространения атаки на другие ВМ через средства взаимодействия, повторное использование ВМ с ранее неправильно настроенной политикой безопасности (так называемые «динамические, мгновенные бреши»), использование типовых ВМ с настроенными политиками безопасности не по назначению);

– угрозы атак отказа в обслуживании, возникающие из-за конфликта ресурсов (т.е. резкое чрезмерное возрастание нагрузки при одновременном выполнении регулярных операций или балансировка, квоты на использование ресурсов хоста) [1], [2].

К специфическим, вытекающим из самой природы облачных вычислений, относятся такие типы угроз, как:

– нарушение конфиденциальности при повторном использовании ресурсов (передача между пользователями типовых виртуальных машин без очистки критических данных (например, ключей к SSH), при распределенном хранении критических данных

(принципиально невозможно локализировать место хранения данных, а иногда (из-за больших нагрузок на аудит) и отследить объемы и направления перемещения данных));

– угрозы атак, использующие размытость границы защищаемой облачной системы (система обычно представлена как портал, куда имеют доступ пользователи с различным уровнем полномочий через незащищенные мобильные терминалы различных типов);

– угрозы атак, использующие слабости криптосистем (при применении облачных технологий многие традиционные криптографические протоколы и методы реализации криптосистем оказываются недопустимыми);

– угрозы атак, использующие слабости систем аудита событий провайдера облачных технологий (поскольку данные хранятся и обрабатываются распределенно, то повышаются требования к системе аудита для прозрачности действий провайдера и требования по защите критических данных пользователей от персонала провайдера);

– угрозы атак, связанные с несанкционированным использованием облачных технологий как средства для осуществления других атак (а именно – для криптоаналитических атак, для хранения и распределения зловредного кода и т.д.).

Перечисленные выше угрозы носят универсальный характер и не зависят ни от функциональности подсистем облачной вычислительной системы, ни от технологии реализации подсистем. Заметим, что отдельные составляющие и подсистемы «облаков» могут быть реализованы и с использованием web-технологий, и с использованием технологий мобильных агентов, в отношении которых существуют свои специфические уязвимости и угрозы. Криптографические и стеганографические системы, построенные по принципу и для облачных технологий наследуют все упомянутые угрозы, поэтому задачи анализа их стойкости, включая стойкость к атакам на реализацию, приобретают новые постановки. Рассмотрим некоторые из них.

Постановки задач. Открытые проблемы

1. Для эффективной работы в составе «облака» криптосистема должна обеспечивать эластичность предоставления услуг, а значит – быть реализованной по одной из технологий, поддерживающих облачные вычисления. В работах [8], [9] авторы предложили технологию реализации криптосистем, которая может применяться для «облаков». Фактически предложенная в них концепция «специальных цифровых носителей информации» является вариантом построения криптосистемы как множества взаимодействующих мобильных агентов. Как в классической агентно-ориентированной парадигме построения распределенных вычислительных систем каждая часть цифрового носителя – интеллектуальный агент, способный подстраиваться под изменяющиеся внешние условия. Наиболее эффективной в этом случае является модель, в которой мобильные агенты, реализующие криптосистему любой сложности, формируются в зависимости от необходимой функциональности из криптопримитивов. Криптосистема, созданная по такому принципу, способна работать с распределенными данными и изменять (как наращивать, так и снижать) свою эффективность без потери стойкости. При этом эффективность оценивается не только быстродействием, но и расходом «ценных» ресурсов (например, случайных последовательностей и ключей). Открытой проблемой является определение минимально достаточного множества криптопримитивов и автоматического определения стойкости криптопротоколов и криптосистем, созданных из этих криптопримитивов. Эта задача повышает также актуальность исследований формального анализа стойкости криптографических протоколов [12].

2. Реализация криптосистем по агентной парадигме может быть осуществлено с использованием XML-шаблонов. Атаки на XML-данные принципиально отличны от атаки на другие форматы хранения данных из-за того, что сами данные содержат

инструкции по их обработке. При этом обработка исключительных ситуаций, ошибок и сбоев тоже, как правило, управляется самими данными в автоматическом режиме. Последнее предоставляет широкие возможности для осуществления атак на реализацию [13]. Открытой проблемой при этом остается отсутствие эффективной по быстродействию формальной методики оценки текущего состояния защищенности от атак на реализацию. Особенно актуальна эта проблема для стеганографичских систем, где до настоящего времени, как известно авторам, такие исследования не проводились.

3. Для распределенных вычислительных систем в общем и для облачных в частности изменяется модель возникновения побочного канала для модулей криптографической защиты информации. В работе [10] главной особенностью такой модели отмечалась возможность моделирования ситуации, когда агенты, составляющие криптосистему, работают на разных узлах распределенной системы. В качестве теоретической основы такой модели рассматривалась общая теория оптимальных алгоритмов [14], [15]. В облачных вычислительных системах добавляются факторы гетерогенности узлов системы, наличия слоя виртуализации и эластичности вычислений. Возникающие при этом побочные каналы отличаются различной природой происхождения (временные, атаки измерения потребляемой мощности, электромагнитных или акустических сигналов, излучаемых при работе модуля КЗИ, утечки информации за счет отсутствия очистки общей памяти и т.д.) и принципиально большей возможностью создания нужных для измерения параметров побочного канала ситуаций (атаки на основе генерируемых ошибок, разностные атаки). Как показали исследования авторов [5], [10], наиболее адекватной математической моделью оценки стойкости криптосистем к атакам с использованием информации из таких побочных каналов является модель, построенная на основании общей теории оптимальных алгоритмов (ОТОА) [14] и ее развитии [15], так как она не требует введения метрики на пространстве параметров побочных каналов, позволяет учитывать неточность и неполноту предоставления информации от различных побочных каналов.

Каждая из перечисленных проблем проектирования и реализации криптосистем (стеганосистем) для облачных вычислений требует отдельного внимания. Остановимся на некоторых аспектах решения задачи оценки стойкости криптосистем к атакам по побочным каналам для облачных вычислений в рамках модели, предложенной в работе [10].

Оценка стойкости к комбинированной атаке по побочным каналам для криптосистем, использующих облачные вычислительные технологии

Рассмотрим пример оценки стойкости криптосистемы, реализующей цифровую подпись по алгоритму RSA, следуя работе [13]. Для сообщения m вычисляется хэш-функция $h(m)$ и подпись $S = h(m)^d \bmod N$, где N – модуль системы RSA, d – секретный ключ выработки подписи, e – открытый ключ верификации подписи, $e \cdot d \equiv 1 \bmod \lambda(N)$, где $\lambda(N)$ – обобщенная функция Эйлера. Предположим, что для вычисления степени используется бинарный алгоритм, а для вычисления остатка по модулю – метод Монтгомери без использования китайской теоремы об остатках. Тогда общая схема алгоритма возведения в степень такова:

Вход: $m, N, d = (d_{n-1},...d_o)_2, h:\{0,1\}^* \to Z/NZ$ Выход: $S = h(m)^d \bmod N$

1. $R_0 \leftarrow 0; R_1 \leftarrow h(m)$

2. For $j = k-1; j \le 0; j--$ do

3. $R_0 \leftarrow R_0^{\;2} \bmod N$

4. If($d_j = 1$) then $R_0 \leftarrow R_0 \cdot R_1 \bmod N$

5. End for Return R_0

Заметим, что при применении метода Монтгомери в результате получаем число в интервале $[0,2N[$ и для получения корректного остатка по модулю требуется одно дополнительное вычитание *N*. В работе [13] рассмотрена следующая схема временной атаки. Атака строится итеративно от старших бит к младшим в предположении, что уже известны старшие биты $d_{n-1},...,d_{n-k+1}$. Цель атаки – установить значение бита d_{n-k}. Предположим, что $d_{n-k} = 1$. Случайно выбираем t сообщений $m_1,...m_t$. Зная $d_{n-1},...,d_{n-k+1},d_{n-k}$ и *N*, можно разбить эти сообщения на два множества: $\mathrm{M}_0 = \{m_i \mid R_0 \cdot R_1 \bmod N$ не требует дополнительное вычитание на шаге 4 алгоритма для $j = n - k\}$ и $\mathrm{M}_1 = \{m_i \mid R_0 \cdot R_1 \bmod N$ требует дополнительное вычитание на шаге 4 алгоритма для $j = n - k\}$. Выбирая сообщения из множеств M_0 и M_1, определяем среднее время выработки цифровой подписи для каждого из множеств – τ_0 и τ_1 соответственно. Если $\tau_0 \approx \tau_1$, то наше предположение $d_{n-k} = 1$ неверно и полагаем $d_{n-k} = 0$. Если $\tau_1 > \tau_0$ и $\tau_1 - \tau_0 \approx \tau_{sub}$, где τ_{sub} – время операции вычитания, то наше предположение верно и $d_{n-k} = 1$.

Оценивая мощность данной атаки, необходимо отметить два важных момента: во-первых, предполагается априорное знание некоторых старших бит ключа, а во-вторых, время выработки цифровой подписи для различных сообщений измеряется в общем случае неточно и зависит от множества случайных факторов. Благодаря этому стойкость криптосистемы к данной атаке зависит от априорной информации и в зависимости от метода ее получения описывается разными моделями и показателями. Это неизбежно приводит к практическим сложностям оценки.

Применим к оценке стойкости криптосистемы к данной атаке на реализацию подход, предложенный в работе [10]. В качестве информационного оператора выбираем оператор $N : \tilde{D} \to X$, где $X = \langle AI, \tau \rangle$, где AI – априорная информация о значении d, τ – информация, полученная из побочного канала по времени, $\tilde{D}$ – множество значений показателя d. Мощность множества $V(N,d) = \{\tilde{d} \in \tilde{D} : N(\tilde{d}) = N(d)\}$ всех элементов $\tilde{d}$, не отличимых с помощью информационного оператора *N* от *d*, определяет принципиальную стойкость к атаке, а радиус информации $r(N)$ и множество алгоритмов реализации атаки – показатель практической сложности ее осуществления. При этом в общем случае оператор *N* всегда неполон, а в зависимости от точности измерения τ – еще и не точен. Показатель стойкости к атаке определяется оператором $S : \tilde{D} \times R_+ \to 2^G$ (в частном случае – функция) утечки информации, G – множество значений функции утечки. С помощью выбора множества $\Phi(N(\tilde{D}))$ алгоритмов реализации атаки описываются такие практические ситуации, как реализуемость алгоритмов прямого перебора по оставшимся неопределенными битам показателя. Тогда условие абсолютной стойкости криптосистемы к атаке определяется как $r(N(\tilde{D})) > 0$, где $r(N(\tilde{D})) > 0$ – радиус информации.

Другим примером применения оценки стойкости на основе ОТОА к анализу стойкости к временным атакам по побочным каналам криптосистем является выбор между

однопроходной и двухпроходной схемой Диффи-Хеллмана при выработке общего ключа для защиты канала обмена сообщениями между мобильным терминалом и «облаком». Учитывая то, что радиус неточной информации для мобильного терминала значительно меньше, чем для «облака», стойкость криптосистемы, функционирующей на мобильном терминале, к временной атаке существенно меньше. Поэтому применение однопроходной схемы Диффи-Хеллмана для мобильных терминалов предпочтительно не только с точки зрения эффективности по быстродействию, но и большей стойкости к атакам на реализацию.

Выводы

Особенности облачной парадигмы построения распределенных вычислительных систем определяет новые постановки задач и порождает открытые проблемы реализации в соответствии с ее принципами криптографических и стеганографических систем. В облачных вычислительных системах добавляются факторы гетерогенности узлов системы, наличия слоя виртуализации и эластичности вычислений. Существующие методики оценки стойкости к атакам на реализацию и методы проектирования криптосистем и стеганосистем [13] не в полной мере применимы в этом случае. Предложенный в статье подход, основанный на применении радиуса информации, позволяет оценивать стойкость к атакам на реализацию, имеющим разную природу возникновения. В качестве примеров рассматриваются оценки стойкости к атаке по побочному временному каналу схемы цифровой подписи по алгоритму RSA и схема распределения ключей Диффи-Хеллмана.

Литература

1. Nick Antonopoulos. Cloud Computing Principles, Systems and Applications / N. Antonopoulos, L. Gillam. – London : Springer-Verlag, 2010. – 379 p.
2. Peter Mell. Effectively and Securely Using the Cloud Computing Paradigm [Электронный ресурс] / Peter Mell, Tim Grance. – Режим доступа : http://csrc.nist.gov/groups/SNS/cloud-computing/index.html
3. Богуш В.М. Перспективи розвитку автоматизованих систем обробки конфіденційної інформації загального призначення / В.М. Богуш, О.А. Довидьков, А.М. Кудін // Вісник Державного університету інформаційно-комунікаційних технологій. – 2003. – Том 1, № 1. – С. 42-46.
4. Кудін А.М. Створення систем підтримки прийняття рішень для управління захистом інформації в хмарних обчислювальних системах / А.М. Кудін // Збірник наукових праць Національної академії державної прикордонної служби імені Б. Хмельницького. – 2010. – № 54. – С. 70-72.
5. Кудин А.М. Алгоритмические аспекты реализации модулей защиты для распределенных вычислительных систем / А.М. Кудин // Вісник Державного університету інформаційно-комунікаційних технологій. – 2011. – Том 9, № 2. – С. 142-147.
6. Harnik D. Side channels in cloud services, the case of deduplication in cloud storage [Электронный ресурс] / D. Harnik, B. Pinkas, A. Shulman-Peleg. – Режим доступа : citeseerx.ist.psu.edu
7. Gentry C. Fully homomorphic encryption using ideal lattice / C. Gentry // Proceedings of the 41st ACM Symposium on Theory of Computing. – STOC 2009. – P. 169-178.
8. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях : навчальний посібник / В.К. Задірака, А.М. Кудін, В.О. Людвиченко, О.С. Олексюк. – Київ ; Тернопіль : Вид. «Підручники та посібники», 2007. – 272 с.
9. О технологии криптографической защиты информации на специальных цифровых носителях / В.К. Задирака, А.М. Кудин, В.А. Людвиченко, А.С. Олексюк // Управляющие системы и машины. – 2010. – № 4. – С. 77-83.
10. Кудин А.М. Модель оценки стойкости модулей криптографической защиты информации к криптоанализу по побочным каналам / А.М. Кудин // Компьютерная математика. – 2011. – № 2. – С. 59-66.
11. Радченко Г.И. Распределенные вычислительные системы / Г.И. Радченко. – Челябинск : Фотохудожник, 2012. – 184 с.
12. Meadows C. Open issues in formal methods for cryptographic protocol analysis / C. Meadows // Proceedings of DISCES 2000. – IEEE Computer Society Press, January 2000. – P. 237-250.

13. Certin Kaya Koc. Cryptographic engineering / Certin Kaya Koc. – Springer Science+Business Media, LLC 2009. – 528 p.
14. Трауб Дж. Общая теория оптимальных алгоритмов / Дж. Трауб, Х. Вожьняковский ; пер. с англ.– М. : Мир, 1983. – 382 с.
15. Трауб Дж. Информация, неопределенность, сложность / Трауб Дж., Васильковский Г., Вожьняковский Х. ; пер. с англ. – М. : Мир, 1988. – 184 с.

Literatura

1. N. Antonopoulos,L. Gillam – London: Springer-Verlag, 2010. – 379 p.
2. Peter Mell, Tim Grance Effectively and Securely Using the Cloud Computing Paradigm // available from http://csrc.nist.gov/groups/SNS/cloud-computing/index.html
3. Bogush V.M., Dovidkov O.A., Kudin A.M. Vesnik derzhavnogo universitetu informatsiyno-komunikatsiynykh tekhnologiy. 2003.Tom 1.№ 1.S. 42-46.
4. Kudin A.M. Zbirnyk naukovykh prats natsionalnoyi akademii derzhavnoyi sluzhby imeni B. Khmelnytskogo.2010.№ 54.S.70-72.
5. Kudin A.M. Vesnik derzhavnogo universitetu informatsiyno-komunikatsiynykh tekhnologiy.Tom. 9.№ 2.2011.S.142-147.
6. D. Harnik, B. Pinkas, A. Shulman-Peleg Side channels in cloud services, the case of deduplication in cloud storage// citeseerx.ist.psu.edu
7. C. Gentry Fully homomorphic encryption using ideal lattice / Proceedings of the 41st ACM Symposium on Theory of Computing. – STOC 2009. – P. 169-178.
8. V.K. Zadiraka, A.M. Kudin, V.O. Lyudvichenko, O.S. Oleksyuk. – Kiyiv-Ternopil: Vyd. “Pidruchnyki ta posibnyki”, 2007.272 s.
9. Zadiraka V.K. Kudin A.M., Lyudvichenko V.O., Oleksyuk O.S. Upravlyayushchiye systemy i mashiny. № 4.2010.S.77-83.
10. Kudin A.M.Kompyuternaya matematika.№ 2.2011.S.59-66.
11. Rachenko G.I. – Chelyabinsk: Fotokhudozhnik, 2012.184 s.
12. C. Meadows Open issues in formal methods for cryptographic protocol analysis / Proceedings of DISCES 2000. – IEEE Computer Society Press, January 2000. – P. 237-250.
13. Certin Kaya Koc. – Springer Science+Business Media, LLC 2009. – 528 p.
14. Dzh. Traub, Kh. Vozhnyakovskiy. – M.:Mir, 1983.382 s.
15. Dzh. Traub, G. Vasilkovsky, Kh. Vozhnyakovskiy. – M.:Mir,1988.184 s.

RESUME

V.K. Zadiraka, A.M. Kudin

Features of the Implementation of Cryptosystems and Stegosystems Based on Clouds Computing

Cloud computing appears to have emerged very recently as a subject of academic interest, but they have become a source new information security problems. Among them there is problem of secure implementation cryptographic and steganographic system. This problem is not solved the existing methods in full.

In the article new method of the cryptosystems and stegosystems security estimation to side-channel attacks is proposed. The offered method is based on general theory of optimal algorithms.

At the first the threats model for cloud computer system is analysis. The specific threats for cryptosystem and stegosystem in cloud are considered. At the second we discuss open problems in implementation of cryptosystems and stegosystems in clouds.

We apply proposed method for analysis security of RSA cryptosystem to well-known timing attacks. We also show preference used information radius for estimation security implementation cryptosystem RSA and one-way Diffi-Hellman scheme in clouds.

Статья поступила в редакцию 08.06.2012.